UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/816,006	03/23/2001	David R. Irvin	8194-492	5173

20792 7590 09/08/2004

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/816,006	IRVIN, DAVID R.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09022004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-50 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-2, 4-11, 13-17, 19-22, 24-26, 28-35, 37-39, 41-48, 50 are rejected under 35 U.S.C. 102(b) as being anticipated by Augustine et al (U.S. 5,440,633).

As per claim 1, Augustine et al discloses generating a random number according to a predetermined random number generation algorithm; constructing a first security field including the random number; encrypting the first security field to create a first digital signature (see column 2 lines 18-28 where the timestamp is the random number); appending the first digital signature to the message to create a packet (see column 2 lines 18-28 where the "management frame" is the same as a packet because a frame has the definition of packet of transmitted information); and transmitting the packet including

the first digital signature and the message (see column 2 lines 29-35 where it is inherent that if an agent receives it had to be transmitted).

As per claim 2, Augustine et al discloses constructing a first security field is preceded by computing a Cyclic Redundancy Check (CRC) for the message, and wherein constructing the first security field comprises constructing the first security field including the first random number and the CRC (see column 2 lines 18-28 where the checksum performs the same function as a CRC).

As per claim 4, Augustine et al discloses the predetermined random number generation algorithm is advanced at the first station with the transmission of each packet (see column 2 lines 18-28 where it is inherent that the time, the random number, will advance with the transmission of each packet).

As per claim 5, Augustine et al discloses receiving the packet including the first digital signature and the message; generating a second random number according to the predetermined random number generation algorithm; constructing a second security field including the second random number; and comparing the second security field including the second random number and the first digital signature (see column 2 lines 29-38).

As per claim 6, Augustine et al discloses encrypting the second security field to create a second digital signature; and comparing the first digital signature and the second digital signature (see column 2 lines 29-38).

As per claim 7, Augustine et al discloses comparing the second security field comprises: unencrypting the first digital signature to obtain the first security field; and comparing the first security field and the second security field (see column 2 lines 39-43 where it is inherent that to obtain the time stamp, the random number, the first digital signature must be unencrypted).

As per claim 8, Augustine et al discloses computing a second Cyclic Redundancy Check for the message portion of the packet; wherein constructing the second security field comprises constructing the second security field including the second random number and the second CRC (see column 2 lines 29-38).

As per claim 9, Augustine et al discloses verifying validity of the message portion of the packet and rejecting the packet if the message is not valid (see column 2 lines 29-43).

As per claim 10, Augustine et al discloses determining if the first digital signature and the second digital signature are the same and rejecting the packet if the first digital signature

and the second digital signature are not the same (see column 2 lines 29-43).

As per claim 11, Augustine et al discloses the predetermined random number generation algorithm and generating the second random number according to the predetermined random number generation algorithm are synchronized so that the first and second random numbers are the same (see column 2 lines 44-54).

As per claim 13, Augustine et al discloses the predetermined random number generation algorithm is advanced at both a first and a second station with the transmission and reception of each packet (see column 2 lines 44-54 were it is inherent that if the clocks are synchronized they must both advance at the transmission and reception of each packet).

As per claim 14, Augustine et al discloses generating at a first station a first random number according to a predetermined random number generation algorithm; constructing at the first station a first security field including the first random number; encrypting the first security field to create a first digital signature; appending the first digital signature to the message to create a packet; transmitting the packet including the first digital signature and the message to a second station; receiving the packet including the first digital signature and

the message at the second station; generating at the second station a second random number according to the predetermined random number generation algorithm; constructing at the second station a second security field including the second random number; and comparing the second security field including the second random number and the first digital signature (see column 2 lines 18-38).

As per claim 15, Augustine et al discloses encrypting the second security field to create a second digital signature and comparing the first digital signature and the second digital signature (see column 2 lines 29-38).

As per claim 16, Augustine et al discloses unencrypting the first digital signature to obtain the first security field; and comparing the first security field and the second security field (see column 2 lines 39-43 where it is inherent that to obtain the time stamp, the random number, the first digital signature must be unencrypted).

As per claim 17, Augustine et al discloses constructing a first security field is preceded by computing a Cyclic Redundancy Check (CRC) for the message, and wherein constructing the first security field comprises constructing the first security field including the first random number and the CRC

(see column 2 lines 18-28 where the checksum performs the same function as a CRC).

As per claim 19, Augustine et al discloses computing a second Cyclic Redundancy Check for the message portion of the packet; wherein constructing the second security field comprises constructing the second security field including the second random number and the second CRC (see column 2 lines 29-38).

As per claim 20, Augustine et al discloses verifying validity of the message portion of the packet and rejecting the packet if the message is not valid (see column 2 lines 29-43).

As per claim 21, Augustine et al discloses determining if the first digital signature and the second digital signature are the same and rejecting the packet if the first digital signature and the second digital signature are not the same (see column 2 lines 29-43).

As per claim 22, Augustine et al discloses the predetermined random number generation algorithm and generating the second random number according to the predetermined random number generation algorithm are synchronized so that the first and second random numbers are the same (see column 2 lines 44-54).

As per claim 24, Augustine et al discloses the predetermined random number generation algorithm is advanced at

both a first and a second station with the transmission and reception of each packet (see column 2 lines 44-54 were it is inherent that if the clocks are synchronized they must both advance at the transmission and reception of each packet).

As per claims 25 and 38, Augustine et al discloses the method and product including a random number generator that generates a random number according to a predetermined random number generation algorithm (the clock); a circuit that constructs a first security field including the random number, encrypts the first security field to create a digital signature, and appends the first digital signature to the message to create a packet; and a transmitter that transmits the packet including the digital signature and the message (see column 7 lines 16-38).

As per claim 26 and 39, Augustine et al discloses the method and product including constructing a first security field is preceded by computing a Cyclic Redundancy Check (CRC) for the message, and wherein constructing the first security field comprises constructing the first security field including the first random number and the CRC (see column 2 lines 18-28 where the checksum performs the same function as a CRC).

As per claim 28 and 41, Augustine et al discloses the method and product including the predetermined random number

generation algorithm is advanced at the first station with the transmission of each packet (see column 2 lines 18-28 where it is inherent that the time, the random number, will advance with the transmission of each packet).

As per claim 29 and 42, Augustine et al discloses the method and product including a receiver that receives the packet including the first digital signature and the message; a second random number generator that generates a second random number according to the predetermined random number generation algorithm; a second circuit that constructs a second security field including the second random number and compares the second security field including the second random number and the first digital signature (see column 7 line 39 through column 8 line 5).

As per claim 30 and 43, Augustine et al discloses the method and product including encrypting the second security field to create a second digital signature; and comparing the first digital signature and the second digital signature (see column 2 lines 29-38).

As per claim 31 and 44, Augustine et al discloses the method and product including comparing the second security field comprises: unencrypting the first digital signature to obtain the first security field; and comparing the first security field

and the second security field (see column 2 lines 39-43 where it is inherent that to obtain the time stamp, the random number, the first digital signature must be unencrypted).

As per claim 32 and 45, Augustine et al discloses the method and product including computing a second Cyclic Redundancy Check for the message portion of the packet; wherein constructing the second security field comprises constructing the second security field including the second random number and the second CRC (see column 2 lines 29-38).

As per claim 33 and 46, Augustine et al discloses the method and product including verifying validity of the message portion of the packet and rejecting the packet if the message is not valid (see column 2 lines 29-43).

As per claim 34 and 47, Augustine et al discloses the method and product including determining if the first digital signature and the second digital signature are the same and rejecting the packet if the first digital signature and the second digital signature are not the same (see column 2 lines 29-43).

As per claim 35 and 48, Augustine et al discloses the method and product including the predetermined random number generation algorithm and generating the second random number according to the predetermined random number generation

algorithm are synchronized so that the first and second random numbers are the same (see column 2 lines 44-54).

As per claim 37 and 50, Augustine et al discloses the method and product including the predetermined random number generation algorithm is advanced at both a first and a second station with the transmission and reception of each packet (see column 2 lines 44-54 were it is inherent that if the clocks are synchronized they must both advance at the transmission and reception of each packet).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3, 18, 27, 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Augustine et al as applied to claims 2, 17, 26, 39 above, and further in view of Xmodem, webkopedia definition (hereinafter Xmodem).

As per claims 3, 18, 27, 40, Augustine et al fails to disclose appending a CRC for the message to the packet.

However Xmodem discloses appending a CRC of the message in a packet (see Xmodem printout where the blocks of data and checksum are functionally the same as a packet with CRC).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to attach the checksum of Xmodem to the packet of Augustine et al's method.

Motivation to do so would have been to allow the recipient of the packet to determine if the message has any errors.

6. Claims 12, 23, 36, 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Augustine et al.

As per claims 12, 23, 36, 49 Augustine et al fails to disclose the use of a common seed to produce the same random number.

Official notice is taken that it is well known that for a pseudorandom number generator to produce the same random number (a step that is essential in the method of verifying the digital signature) the same seed must be used.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Handbook of

Applied Cryptography discloses the use of a system clock for generating random bits and Kravitz (U.S. 5,231,668) discloses the same the method of creating the digital signature as disclosed by the applicant.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:30am - 5:00pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell
Andrew Caldwell

MJP